AU/SCHOOL/NNN/2004-04

PROGRAM ON INFORMATION RESOURCES POLICY

HARVARD UNIVERSITY, CAMBRIDGE, MASSACHUSETTS

AIR UNIVERSITY

LEAKS IN THE NATIONAL INFORMATION INFRASTRUCTURE DAM:

WHO SHOULD PROTECT IT?

by

Curtis O. Piontkowsky, Lt Col, USAF

A Research Report Submitted to the Air University Faculty
In Partial Fulfillment of the Graduation Requirements

Advisor: Dr. Anthony G. Oettinger
Chairman, Program on Information Resources Policy
Harvard University, Cambridge, Massachusetts

Maxwell Air Force Base, Alabama
April 2004

Report Documentation Page

Report Documentation Page	Form Approved OMB No. 0704-0188

Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.

1. REPORT DATE **APR 2004**	2. REPORT TYPE **N/A**	3. DATES COVERED **-**
4. TITLE AND SUBTITLE **Leaks in The National Information Infrastructure Dam: Who Should Protect It?**		5a. CONTRACT NUMBER
		5b. GRANT NUMBER
		5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)		5d. PROJECT NUMBER
		5e. TASK NUMBER
		5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Air University Maxwell AFB, AL**		8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)		10. SPONSOR/MONITOR'S ACRONYM(S)
		11. SPONSOR/MONITOR'S REPORT NUMBER(S)
12. DISTRIBUTION/AVAILABILITY STATEMENT **Approved for public release, distribution unlimited**		
13. SUPPLEMENTARY NOTES		
14. ABSTRACT		
15. SUBJECT TERMS		

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**UU**	**56**	

Disclaimer

The views expressed in this academic research paper are those of the author and do not reflect the official policy or position of the US government or the Department of Defense. In accordance with Air Force Instruction 51-303, it is not copyrighted, but is the property of the United States government.

Contents

Page

Illustrations

Page

Preface

Is the national information infrastructure vulnerable? What's the government's role in protecting it? This topic is timely and timeless. As more of our daily lives are conducted on-line, my concern for information security—integrity, authentication and non-repudiation—coupled with the privacy of our individual and collective data led me to examine this arena. What became evident from the onset is the unending requirement to continually examine the vulnerabilities of our constantly evolving, interconnected networks and take prudent measures, both public and private, to ensure the continued viability of cyber space for national defense, financial interactions and commercial activities.

I owe sincere thanks and appreciation to those generous enough to provide guidance and assistance. A heartfelt, thank you to Dr. Anthony Oettinger, Chairman of the Harvard University Program on Information Resources Policy without whose help I could not have completed this report. Thanks to my family for their patience and understanding throughout. I also want to thank Harvard University Professors Jean Camp for her course on Security and Privacy and Marie Danziger for guidance on research preparation and writing techniques. Those people who assisted and the Program on Information Resources Policy affiliates, however, are not responsible for or necessarily in agreement with the views expressed herein, nor should they be blamed for any error of fact or interpretation.

Abstract

Are our interconnected, electronic media and communications so pervasive, so entwined in our national defense, our economy, and our way of life that its demise would bring down the nation? What responsibilities does the government have for protecting this 'environment'? This paper examines:

- The responsibilities of government
- Why the national information infrastructure needs protecting
- What the nation has done
- The nation's options for the future

Rapid growth and commercialization since the Internet's inception, and an under appreciation for security opened the floodgates for problems—from fraud and theft to defacements, disruptions, and denial of service attacks. In order for the national information infrastructure to sustain its crucial position in a wide range of essential activities it must be secure (physically and electronically). This study reviews government's role and responsibilities for policy, security, standards, laws and partnerships with the private sector. My assessment is that the governmental policy framework is well established, security is being pushed to the forefront of our national consciousness, and standards continue to evolve. Legislation placing additional responsibility and liability for Internet security upon software and hardware developers, ISPs, corporations and individuals may be a prudent next step. Simultaneously, government should complement legislation with incentives (e.g. tax breaks and subsidies)

to encourage the private sector to establish and maintain a secure environment for essential Internet activities to operate.

Chapter 1

What are the responsibilities of government?

If men were angels, no government would be necessary.

—James Madison

The United States' Constitution says:

> We the People of the United States, in Order to form a more perfect Union, establish Justice, insure domestic Tranquility, provide for the common defense, promote the general Welfare, and secure the Blessings of Liberty to ourselves and our Posterity, do ordain and establish this Constitution for the United States of America.[1]

Since one of the foundations of the United States government is to provide for the common defense, shouldn't that extend to the defense of cyberspace? The most basic responsibility of Government is national survival—the common defense. Are the interconnected, electronic media so pervasive, so entwined in our national defense, our economy, and our way of life that its demise would bring down the nation?

Review of any basic government textbook indicates the national government has sole responsibility to print money, regulate interstate and international trade, make treaties and conduct foreign policy, declare war, establish and maintain the military and make laws essential to carrying out governmental responsibilities. Government responsibility is the struggle to maintain a balance between liberty and order by restricting behaviors that harm others. All of government's responsibilities require responsible partnership with the private sector and corporate actors, coupled with individual responsibility. The national information infrastructure (NII) plays a role in the economy, interstate and international trade, national defense, and it is the focus of international discussion and cooperation. The NII plays a central role in numerous studies, papers and books about Cyber War. All the tentacles of the NII encircle and interface between and among the various public and private sector realms. The pervasive nature of the NII and our growing dependency upon its capabilities clearly indicates its demise would be extremely detrimental to our nation.

Notes

[1] The Constitution of the United States, http://www.archives.gov/national_archives_experience/constitution_transcript.html

Chapter 2

What is the National Information Infrastructure?

> *When I took office, only high-energy physicists had ever heard of what is called the Worldwide Web.... Now even my cat has its own page.*
>
> —William J. Clinton

The "national information infrastructure" is a term coined by the government describing the continuing integration of information and telecommunications technologies. The fact government coined a term to describe this infrastructure illustrates how pervasive computers and internet technology have become in almost all facets of our modern life—travel reservations and stock transactions, online shopping and banking, obtaining information from phone numbers to directions, research and online gaming … the list goes on.

In literature, legislation, and practice people lump a wide variety of entities under the rubric of the national information infrastructure. Let's take a look at a few historical examples. In 1993, the Information Infrastructure Task Force[1] tried to clarify the discussion, stating the national information infrastructure is *"a seamless web of communications networks, computers, databases, and consumer electronics that will put vast amounts of information at users' fingertips."*[2] A letter from Vice President Gore, provided the additional promise of a seamless web *"of communications networks including computers, televisions, telephones and satellites"*... expected to continuously alter the way Americans *"live, learn, work and communicate with each other both in the United States and around the world."*[3]

In 1996, President Clinton established the President's Commission on Critical Infrastructure Protection. The Executive Order stated, "*Certain national infrastructures are so vital that their incapacity or destruction would have a debilitating impact on the defense or economic security of the United States.'*[4] The included infrastructures were telecommunications; electrical power systems; gas and oil storage and transportation; banking and finance; transportation; water supply systems; emergency services (including medical, police, fire, and rescue); and, continuity of government. In 1998 a Presidential Decision Directive[5] and the Department of Defense Critical Information Infrastructure Protection Plan maintained this focus, indicating critical infrastructures are the physical and cyber-based systems essential to the minimum operations of the economy and government—*"so vital to the Nation that their incapacity or destruction would have a debilitating impact on national security, national economic security, and/or national public health and safety*."[6]

The National Strategy to Secure Cyberspace, 2004, identified infrastructures similar to hose outlined by President Clinton's 1996 Executive Order and highlighted the integrated nature of cyberspace—the interconnected computers, servers, routers, switches, and fiber optic cables—the 'nervous system' of all the infrastructures that serve as the country's 'control system.'[7] We will focus on this cyberspace—commonly referred to as the Internet—portion of the national information infrastructure and take a brief look at the essential supporting infrastructures of energy and telecommunications.

We normally think of our national information infrastructure as a series of interconnected, interwoven systems. However, it's important to understand not every system is interconnected or interdependent. Yes, every day capabilities change and additional ones are added. Yes, each new interconnected capability adds additional threats, vulnerabilities, and susceptibilities. But, each addition may also add redundancy and potentially enhance robustness and resiliency. This globally connected system of systems provides wide-ranging capabilities. We have access to immeasurable volumes of information and access to a wide variety of control systems. But, not everything is "connected." There is a trade-off between functionality and security. If we have a system where security is of the utmost importance then couldn't we eliminate or reduce the global connectivity and isolate the system? Of course there may be a price of reduced capability to enhance security.

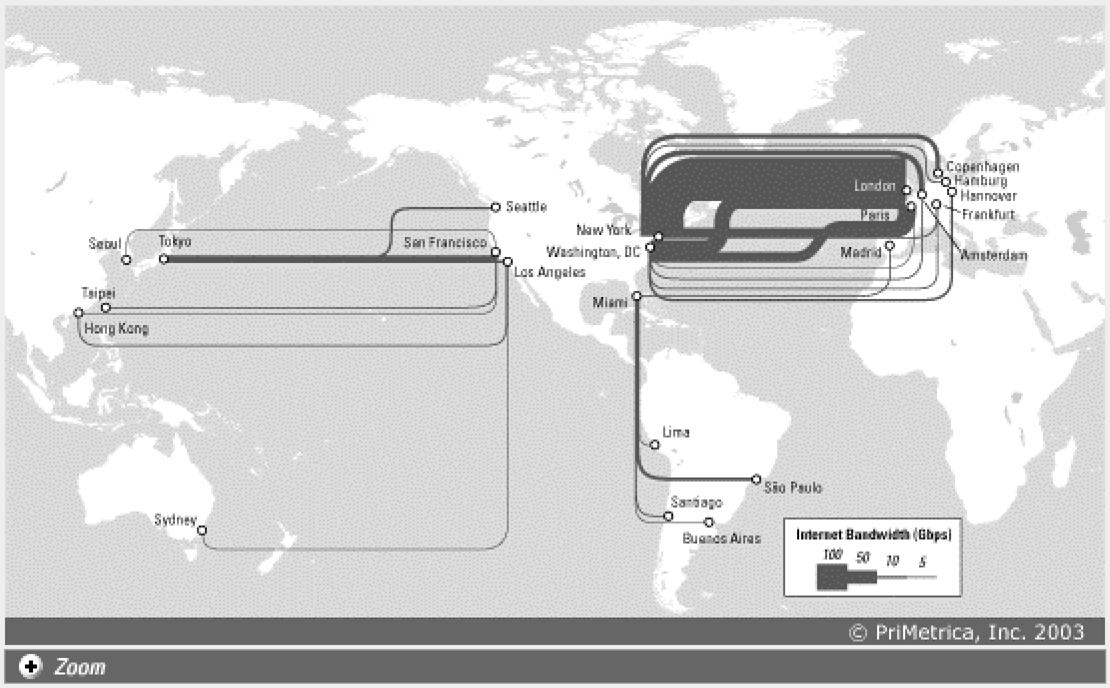
We've limited our focus primarily to the Internet, with a brief look at the supporting telecommunications and electrical power infrastructures. Our line of consideration is, for the most part drawn above the individual user. However, individual users are an important consideration in systems security and create significant risks. Thus, this should be considered a "fluid" boundary—where responsibility lies.

What is the Internet?

In 1995 the Federal Networking Council (FNC) described the Internet as, "a global information system … not only the underlying communications technology, but also higher-level protocols and end-user applications, the associated data structures and the means by which the information may be processed, manifested, or otherwise used." This definition provides many parallels to the image of the Internet as an 'information superhighway.' Similar to the federal highway system—concrete lanes, bridges, rest areas, on and off ramps and, essential supporting physical and informational infrastructure—signs, maps, maintenance, snow removal, speed limits, and related services and products (e.g. service plazas and fuel), the Internet has levels of access, and differing levels of service."[8]

The Internet is a global series of packet-switched networks using a standardized set of protocols. The end users 'on ramp' to the Internet is normally through an Internet Service Provider (ISP). Network Operation Centers (NOCs) manage high capacity networks for large ISPs. They link the ISPs together through Internet peering points or network access points. Smaller ISPs typically lease long-haul transmission capacity from larger ISPs and then provide end users Internet access via the Public Switched Telephone Network (PSTN). The Internet access providers connect to the PSTN through points of presence—normally a switch or a router in a carrier's central office. Figure 1 illustrates international Internet traffic, like other PSTN transmissions, traveling to and from the United States primarily via underwater cables and satellites.[9]

Map of Major Interregional Internet Routes, 2003

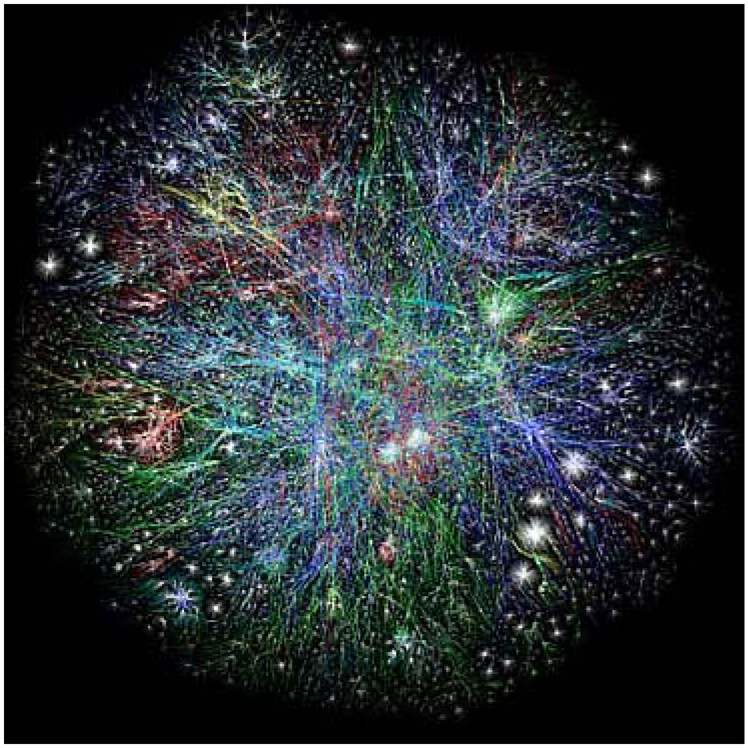


Notes: Map includes interregional Internet routes with at least 2.5 Gbps of aggregate capacity. Figures represent Internet bandwidth connected across international borders to each Consolidated Metropolitan Statistical Area or equivalent. Domestic routes are omitted. Data as of mid-2003.

Source: TeleGeography research http://www.telegeography.com/ee/free_resources/gig2004-03.php	© PriMetrica, Inc. 2004

Figure 1 Map of Internet Routes

Clearly the Internet is a dynamic array of systems—the United States has 7,800 ISPs and 166 million Internet users—which we can expect to continue to increase and evolve.[10] Figure 2 illustrates the global ‘explosion’ of Internet capability in a color map representing the different world regions by differing colors. This array is best viewed in color at the web site (www.opte.org/maps), to differentiate among the different regions around the globe.



Each color on this Opte map represents a region; North America, blue; Europe/Middle East/Central Asia/Africa, green; Latin America, yellow; Asia Pacific, red; Unknown, white. (Image: Opte.org)
The Opte Project – www.opte.org/maps

Figure 2 Color Map Representing the Internet

Some people prescribe the Internet as the magic potion for everything—economists predict substantial increases in productivity, efficiency and prosperity; businesses and entrepreneurs anticipate large gains and new market share from on-line business and an increasing consumer preference to shop from home via the Internet.[11] It seems as though the Internet connects 'everything' to 'everything else' while maintaining connectivity even when nodes and links fail.

Notes

[1] The White House formed the Information Infrastructure Task Force (IITF) in 1993 to articulate and implement the Administration's vision for the National Information Infrastructure (NII)

[2] Byon, I., *Survivability of the U.S. Electric Power Industry*, Master of Science in Information Networking, 2000, Carnegie Mellon University

Notes

[3] ibid

[4] Executive Order 13010, July 15, 1996

[5] Presidential Decision Directive/NSC-63, *Critical Infrastructure Protection*, May 22, 1998

[6] Department of Defense *Critical Information Infrastructure Protection Plan*, November 18, 1998

[7] *The National Strategy to Secure Cyberspace*, 2004

[8] Kahn, Robert E. and Cerf, Vinton G., Internet History, *What Is The Internet (And What Makes It Work)*, 1999

[9] The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets, 2003, Submarine cables and global internet map at: http://www.telegeography.com/maps

[10] CIA World Factbook: United States, 2002, Federal Information and News Dispatch, Inc.

[11] *The Economist: Internet security-Combating hooligans in online space*, 2003, http://www.ebusinessforum.com/index.asp?layout=rich_story&doc_id=6869

Chapter 3

Why does the National Information Infrastructure need Protecting?

> *Programming today is a race between software engineers striving to build bigger and better idiot-proof programs, and the Universe trying to produce bigger and better idiots. So far, the Universe is winning.*
>
> —Rich Cook

Why does it need protecting?

Most of us have heard some version of American writer Mary Mapes Dodge's fable about the little Dutch boy who finds the leak in the dike and spends all night alone, in the cold and dark plugging it with his thumb. If we imagine the national information infrastructure as one large leaky dike and un-orchestrated individual efforts to hold back the flood of problems—viruses, worms, web bugs and Trojans, "logic bombs," distributed denial of service attacks, and direct attacks against the Domain Name System, plus hackers, crackers, phishers, spies, terrorists, and determined mischief makers of all kinds, coupled with irritating intrusions (spam, popup ads, spyware, etc.)—then we begin to see how daunting a task it is to "protect the national information infrastructure." But, does it need protecting? A survey conducted by the Pew Internet and American Life Project, released in August 2003, indicates almost half of Americans believe terrorists will launch a cyber attack on our businesses and utilities.[1]

Some people say there is 'no problem' and others overstate the problem. We've heard the minimalist or 'easy' technical cures—anti-virus software, additional hardware (e.g. firewalls) and improved software security can solve all our problems; just a bit more technical expertise and we'll stop these attacks. We've also heard the "Chicken Little, the sky is falling" version of threats—sometimes over-hyped and emotional—"we can't do enough to stop the onslaught." Both views have some basis in fact, yet neither is absolute. Let's look at these differing views and the underlying threats, vulnerabilities, and susceptibilities.

It's not even raining: there is no problem

A research paper released in December 2002 by the Center for Strategic & International Studies (CSIS), a Washington-based think tank, disputes the seriousness of the threat from cyber terrorism postulated by the government and the media. It argues that the assumption of vulnerability is wrong because computer networks and critical infrastructures are distinct concepts. James A. Lewis, a CSIS analyst and author of *Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats* explains that although many computer networks remain vulnerable to attack, very few critical infrastructures are equally vulnerable.[2] Since banking and financial transactions occur through separate networks (e.g. SWIFT and CHIPS), attacks impacting these transactions would require substantial insider access and a lot more effort and risk to plan and implement than comparable assaults on the open Internet.

Kevin Terpstra, former communications director for the California Department of Information Technology (the agency that was responsible for assessing the security of the state's computer systems), said, "The notion that somebody armed with a laptop in

Peshawar, Pakistan, could bring down California's power grid is pretty far-fetched." He did indicate there is reason to be concerned about computer security and critical infrastructure vulnerabilities, but stressed the likelihood of this type of an attack is very small."[3]

Declan McCullagh, Chief political correspondent for CNET News.com, believes the perception of the threat of cyber terrorism is askew. He points to the historical facts that most devastating terrorist acts have been physical attacks—the Marine barracks in Lebanon, the U.S.S. Cole, the Oklahoma City federal building, the World Trade Center and the Pentagon—not keyboard toting hackers. He summarizes his point stating, "We don't need any more government officials clamoring for intrusive new laws and claiming, against all common sense, that a 'digital Pearl Harbor' is just around the corner."[4]

The sky is falling: an overwhelming problem

A paper presented at the 11th USENIX Security Symposium infers that the ability of attackers to rapidly gain control of an enormous number of Internet hosts poses an immense risk to the overall security of the Internet. The authors postulate that a surreptitious worm, self-propagating throughout the Internet by exploiting security flaws in commonly used services, could easily subvert a million or possibly even ten million Internet hosts. These hosts might then be employed for nefarious activities such as launching massive denial of service attacks, stealing or corrupting great quantities of sensitive information, and other more subtle activities to confuse and disrupt use of the Internet. Epidemic proportioned attacks could cripple e-commerce sites, news outlets, command and control infrastructure, specific routers, or the root name servers. Further, the ability to control all those hosts would provide direct access to any sensitive information stored on those millions of computers—corporate research, strategies and plans, customer information, passwords, credit card numbers, financial records, address books, archived email, and patterns of user activity. Not only can the information be accessed, but also corrupted and sent out from the specific user's own computer. The potential for damage to a computerized, Internet-driven nation and economy is on the scale of warfare or massive terrorism.[5]

Dr. Martin Libicki, a Senior Policy Analyst at RAND Corporation struck a similar chord, indicating, "The potential consequences of deliberately induced systems failure or corruption are vast." He suggests that if computer attackers controlled the key systems that underpin our society they could, theoretically, listen to phone calls, misroute connections, and stop phone service entirely; shut down electrical power; interfere with financial transactions totaling trillions of dollars weekly; hinder emergency services; delay U.S. military responses to crises abroad; disclose personal medical information; interfere with transportation systems; and lots more. Day-to-day activities of our interconnected society would come to a stand still.[6]

So, is there a problem? The National Strategy to Secure Cyberspace emphasizes the dependency of the U. S. economy and national security on information technology and the information infrastructure. The central component of this information infrastructure is the Internet—a network initially designed to share unclassified research among scientists. Today there are millions of computer networks connected to the Internet. *The National Strategy to Secure Cyberspace* indicates many of the nation's essential services and infrastructures are integrated and/or controlled via the Internet—not just information but physical structures (e.g. nuclear power plants, electrical transformers, air traffic control systems, trains, dams, pipeline pumps, chemical vats, radars, and stock markets). The Strategy says a wide variety of "*malicious actors can and do conduct attacks against our critical information infrastructures...*" and highlights concerns over "*the threat of organized cyber attacks.*"[7]

Some information security professionals agree. Dan Geer—formerly of the security firm @ stake Inc.—took an example from biology and postulated the software 'monoculture' cultivated by Microsoft is a threat to global computer security. He believes a computer virus capable of exploiting a single flaw in the Microsoft operating systems could wreak havoc, just like a virus impacting any species with a shared weakness could have widespread results.[8]

President Decision Directive 63 discusses the transition of the nation's critical infrastructures from physically and logically separate, independent systems through information technology advances and improved efficiency to increased automation and connectivity. These advances opened up new susceptibilities—to equipment failure, human error, weather and other natural causes, and physical and cyber attacks.[9] The PDD established a national structure for CIP illustrated below (Figure 3). A number of these organizations and responsibilities have been transferred to the Department of Homeland Security.

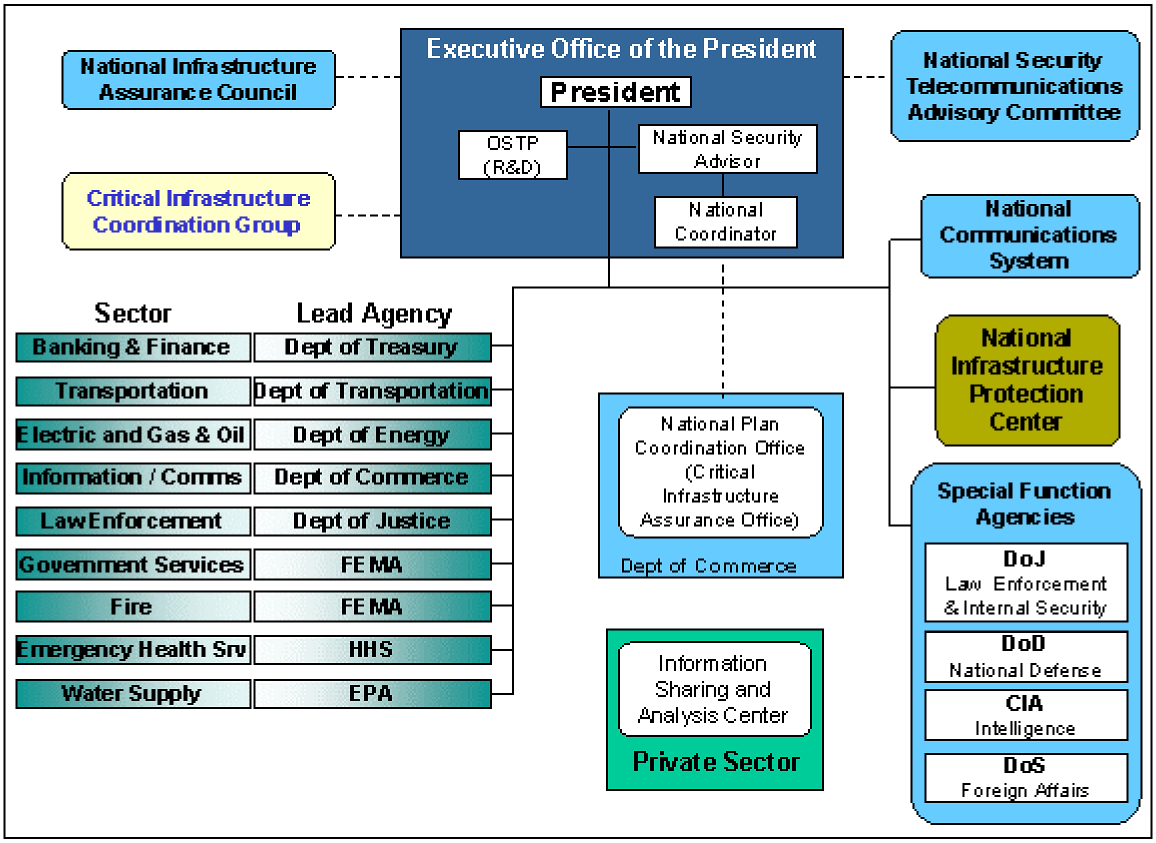


Figure 3 National Structure for Critical Infrastructure Protection

Threats, Susceptibilities, and Vulnerabilities

Information security professionals promoting their services, sales people marketing firewalls and anti-virus software, and university professors searching for industry grants all have incentives to overstate the threat. ISPs who want their customers to spend hours on-line and software companies have reasons to understate the vulnerabilities.[10]

Although both 'no problem' and 'overwhelming problem' could be assessed to have some partial validity, neither is the absolute truth. Those who think there are no problems aren't paying attention. Those who assert the problems are completely unstoppable are also in the extreme. However, we must acknowledge there is a problem. The problem consists of threats, vulnerabilities and susceptibilities to the Internet and supporting infrastructures. First let's outline what we mean by threats, vulnerabilities and susceptibilities then take a more detailed look at the sources, costs and problems.

Threats.

"*Threats are the actors that can cause damage to information resources. They may be categorized into chance events (fires, earthquakes, utility outages), hostile agents (insiders or outsiders who have specific hostile intent towards a[n] information resource, and non-hostile agents (the incompetent and incapacitated), and agents hostile to someone else – or to no one in particular, such as authors of computer viruses and worms.*"[11]

Susceptibilities.

"Susceptibilities represent the openness of an information resource to damage of some kind regardless of the threat."[12]

Vulnerabilities.

"A v*ulnerability is a combination of 1) threats that act to cause damage, and 2) susceptibilities to actions that allow such damage to occur."*[13]

Sources and Costs of Attacks

We know portions of the 'digital world, become more interconnected every day. More and more of our lives are conducted "on-line"—purchases and payments to instant messaging and collaboration. This easy access provides convenience and speeds for many of our activities, but it also makes our information and us more vulnerable.

We know industries and services are vulnerable to a variety of threats, running the gamut from kiddie hackers to cyber war. Soft attacks against poorly designed hardware—firewalls and servers—and software code, as well as nodes subject to physical attacks from rogue governments, terrorist organizations and others intent on disrupting our society.

Statistics, surveys and experience show us there is reason for some concern. Respondents to the CSI/FBI 2003 Computer Crime Survey identified independent hackers as the most likely source of attacks against their networks (Figure 4).

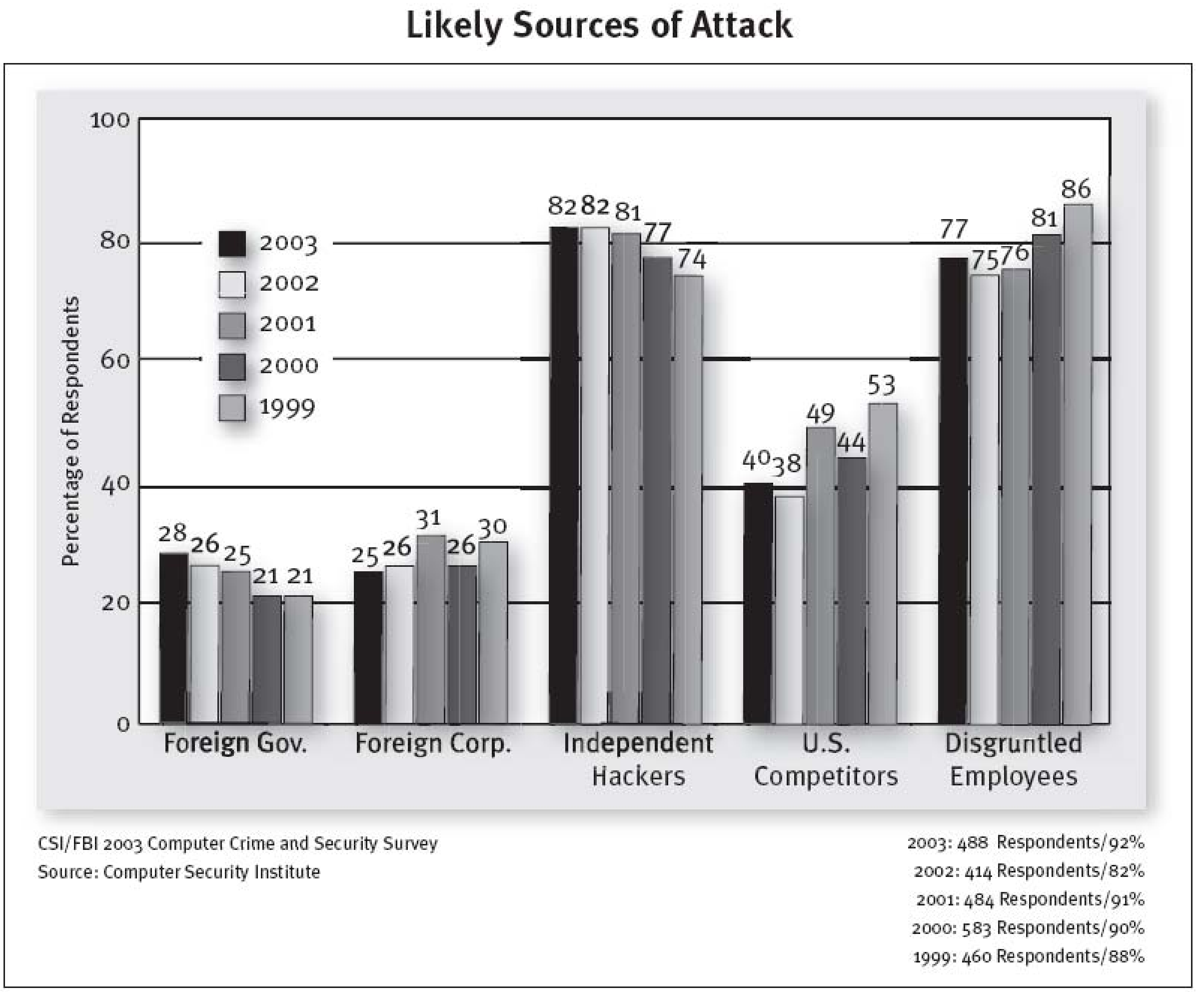


Figure 4 Likely Sources of Attacks[14]

Most intrusions and attacks exploit known vulnerabilities, configuration errors, or virus attacks where countermeasures were available.[15] These attacks can come from "outsiders" or insiders." An insider is someone we give access to our data or networks or who has bypassed security measures to designate themselves as an "insider," while an outsider is someone determined enough to locate and take advantage of the weaknesses in our controls, encryption, firewalls and software.

Whatever the method and whoever the attacker, there is always the potential for significant losses due to financial fraud, theft of proprietary information, viruses, insider network abuse, sabotage, etc. Respondents to the 2003 CSI/FBI survey reported more than $200 million in overall financial losses (Figure 5) from just 47% (251 of 530) of survey respondents.

Dollar Amount of Losses by Type

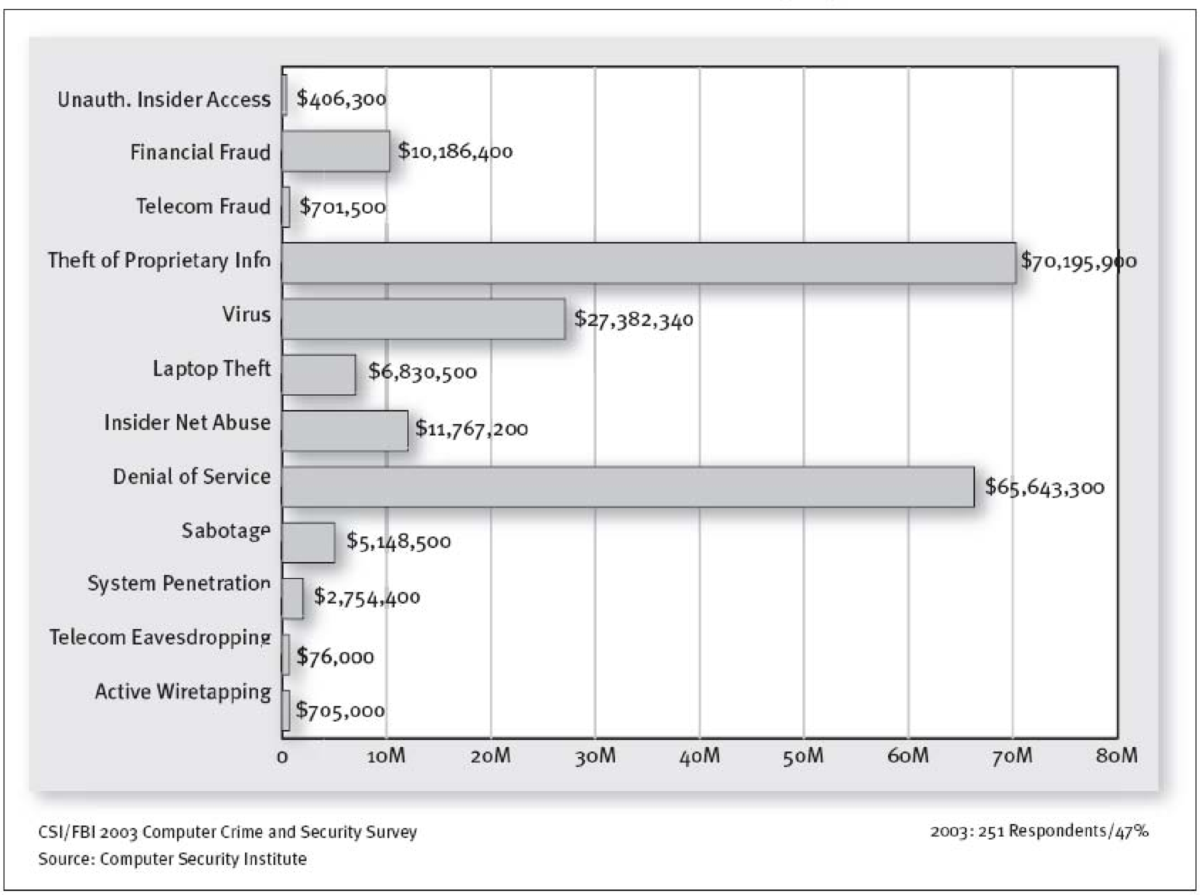


Figure 5 Dollar Amount of Losses by Type

We know there are attacks and we know they are costly. The most likely threats seem to be cyber threats, physical threats, and insider sabotage.

Cyber Threats

Computer attacks are a serious problem. In 2002, the CERT/CC reported 82,094 computer security incidents and 4,129 distinct vulnerabilities reported; by 2003 these numbers rose to 137,529 incidents and 3,784 vulnerabilities.

PDD-63 identifies specific reasons for the likelihood of a cyber attack—our military strength and our economies increased reliance on the national information infrastructure. These reasons should be enough to keep the nation focused on the continuing need to prepare for current and future attacks. Amit Yoran, the director of the U.S. Department of Homeland Security, National Cyber Security Division, compared current assessments minimizing the threat of future cyber terrorist attacks to the early days of military air power—when the use of air power in war was thought to be ineffective. "We need to be thinking about how today's advances in cyberspace can be turned against us." Even though most cyber attacks so far have been unsophisticated and predominantly criminal in nature, "we cannot count on that forever or even for long."[16]

Statistics indicate his concerns are valid. The CSI/FBI Survey indicates nearly steady rates in the types of attacks and misuse reported over the past 5 years (Figure 6). Since these numbers aren't going down significantly, we can surmise the likelihood of a significantly greater attack is coming—it's just a matter of when.

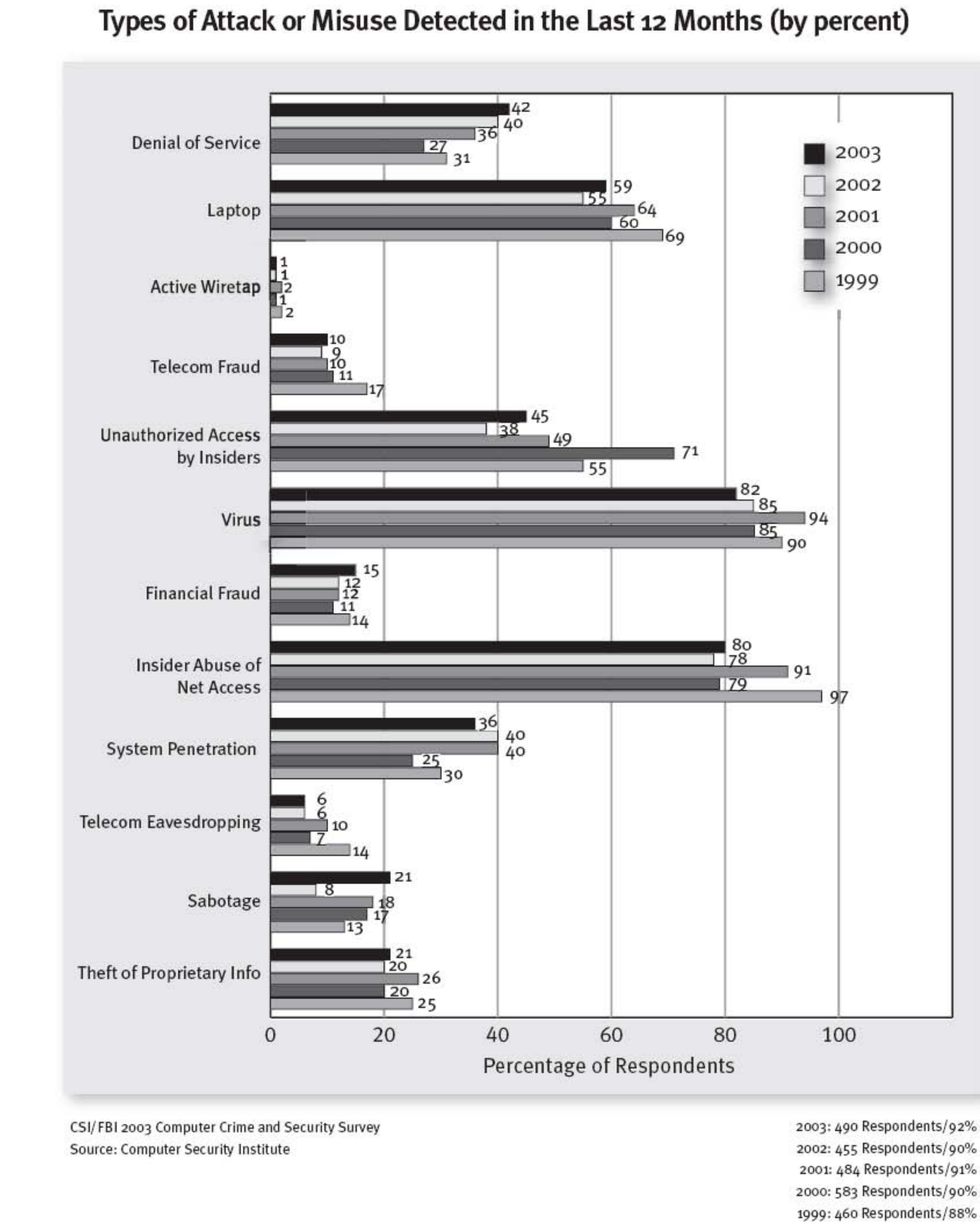


Figure 6 Types of Attacks Detected

It is a commonly held belief that it requires a significant level of technical sophistication to carry out a debilitating cyber attack. So far, sustained, devastating attacks have not occurred. Is this, at least in part, due to our enemies lacking the necessary technical skills? We should not let the assessment of an apparent lack of capability lull us into a false sense of security.[17] The methods and tools for cyber attacks are becoming more readily available. Some hacking tools can be downloaded from the Internet along with instructions. In 2002 American spies in Pakistan found an alleged al-Qaeda hacker training center focused on breaking into the computer systems of dams, power grids and nuclear plants.[18] The CERT Coordination Center chart below (Figure 7) indicates that the sophistication of attacks is rising while the intruder knowledge required to carry them out is decreasing.

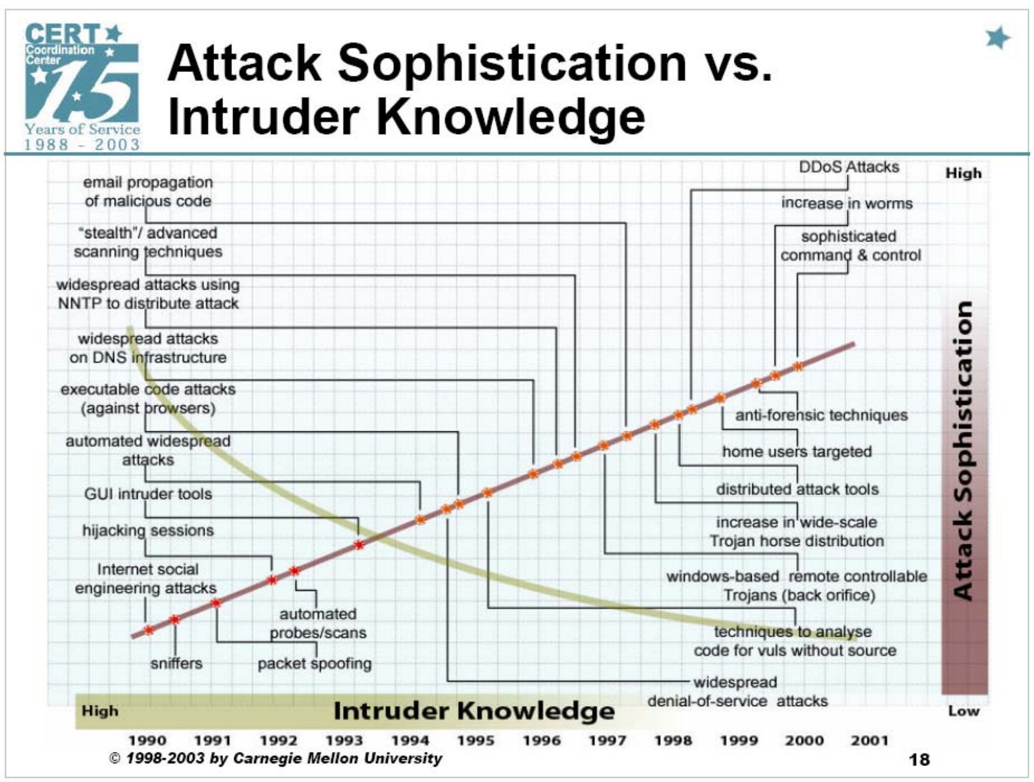


Figure 7 CERT/CC Chart of Attack Sophistication vs. Intruder Knowledge[19]

While the knowledge required to carry out attacks may be decreasing, there is a high probability (and some empirical evidence) that our enemies are conducting espionage against our Government, university research centers, and private companies. It's possible they are mapping our national information infrastructure systems, singling out key targets, and working to infiltrate our systems with 'back doors' and other serendipitous means of access for cyber attacks.[20]

Internet attacks from various cyber threats remain fairly easy, difficult to trace, hard to prosecute and a low risk for the attacker. Cyber threats can be aligned into five primary categories that impact key components of the Internet—Denial of Service, Worms, Domain Name Server, against and using routers, and cyber crime.[21]

Distributed denial of service.

Denial of service attacks employ automated attack tools to allow an attacker to control thousands of compromised systems and strike at one or more victim systems. Since the Internet is a finite, interdependent resource—bandwidth, transmission, routing and switching equipment, denial-of-service attacks can be effective. [22] In one of the most recent denial of service attacks, the Recording Industry Association of America was attacked by the MyDoom.F virus and offline for 5 days in March 2004.

Denial of service attacks have become high-impact, low-effort operations for attackers. Cooperative Association for Internet Data Analysis estimates an average of 4,000 denial-of-service attacks hit the Internet each week. The bandwidth of most organizations Internet connections is normally between 1 and 155 megabits per second

(Mbps). Attacks exceeding hundreds of Mbps have been reported—enough to inundate almost any system on the Internet.[23]

Worms

Worms are self-propagating malicious code. Their automated nature and the relatively widespread nature of the vulnerabilities they exploit could allow a large number of systems to be compromised in a short period of time. The Code Red infected more than 250,000 systems in just 9 hours on July 19, 2001. "*Worms can include built-in denial-of-service attacks. The traffic they generate can also create a denial of service effect. They have the potential to crash routers, overload ISPs, and cause printers to crash or print junk.*"[24]

The Blaster worm and the SoBig virus caused losses estimated at $35 billion during the summer of 2003. These attacks seem to indicate less emphasis on viruses that require some human intervention to spread and more on worms that attack through unprotected connections to the network without any direct human intervention. Worms represent an extremely serious threat to the safety of the Internet. Recent worms have infected hundreds of thousands of hosts within hours. "Better engineered worms could spread in minutes or even tens of seconds rather than hours, and could be controlled, modified, and maintained indefinitely, posing an ongoing threat of use in attack on a variety of sites and infrastructures."[25]

Attacks on the Internet Domain Name System (DNS)

"The Domain Name System is the dispersed, hierarchical global directory that translates names (www.comcast.net) *to numeric IP addresses* (204.127.205.8). *The top 2 layers of the hierarchy—13 'root' name servers* (10 in the US and 3 outside at

undisclosed locations) *in the top layer coupled with the 'top level domain' (TLD) servers (authoritative for ".com", ".net", etc.), as well as the country code top level domains (ccTLDs – ".us", ".uk", ".de", etc.)—are critical to the operation of the Internet."*[26]

The DNS was attacked in October 2003. A distributed denial of service attack, that lasted one hour, targeted seven of the 13 root servers. The servers were flooded with fake traffic from a large number of hijacked "slave" machines. The servers were inundated with up to 40 times their normal traffic load. The attack went virtually unnoticed by the majority of Internet users. One security expert suggested it would take at least four hours of continuous attack for traffic to be slowed noticeably, because a host of secondary domain name servers, rather than the 13 root servers routs most web traffic.

Attacks against or using routers

Cyber threats associated with routers include:

- poorly secured routers used as attack platforms to generating attack traffic at other sites
- Denial of service by directing a larger amount of traffic at routers rather than through them
- modifying, deleting, or inserting erroneous routes into the global Internet routing tables to redirect traffic destined for one network to another[27]

In 2001, Weather.com was hit by a denial-of-service attack that shut down operations for several hours when the routers of its hosting facility, operated by Exodus, were clogged with bogus traffic.

Cyber crime

Although not specifically a direct attack on the information infrastructure, cyber crimes—extortion, phishing, remote theft of data, economic espionage, credit card swindles, etc.—can be the criminal culmination of one or more cyber attacks or covertly embedded cyber attack capabilities.

Banks, brokerage houses, and investment firms in the United States and the United Kingdom have paid off cyber criminals who threatened to attack their computer systems and destroy their data unless a 'ransom' was paid. These cyber extortionists left encrypted messages and remotely crashing senior directors systems to demonstrate their capability to make good on threats. Four incidents reportedly occurring in London, indicated firms transferred money to an offshore bank account to meet the ultimatums. Other incidents include:

- intruders demanded a large ransom after they stole a major credit card company's computer source code and threatened to crash their entire system; and
- a cyber criminal stole more than 300,000 credit card numbers from an online music company and demanded a $100,000 ransom. When they refused to pay, the numbers were publicly posted.[28]

Damage assessments for these attacks are inexact—except for specific ransoms—but there are estimates global corporations could lose millions of dollars if their systems crashed for just one day. This type of crime receives very little publicity. Corporations and officials fear publicity could cause customers to lose confidence in their ability to protect sensitive financial data and result in additional occurrences.[29] The detrimental impact on customer confidence and trust is immeasurable.

Although they capture the news headlines, crime syndicates and terrorists are not the only ones attacking through cyber space. Bruce Schneier, Founder and the Chief Technical Officer of Counterpane Internet Security, Inc., believes the vast majority came from inside the United States. *"Less than 1% of recent computer attacks originated in countries that America considers breeding grounds for terrorists. Hackers are more* *likely to be* [disgruntled or dishonest employees], *geeky teens on an ego trip, or greedy crooks hoping to steal money online, than Islamic fundamentalists."*[30]

Cyber attacks can take a wide variety of approaches and come from a large list of potential actors. They are, primarily, against specific targets—segments of the internet, corporations, military or government entities; however they can also be used against control systems supporting other segments of the national information infrastructure.

These examples and the alerts and warnings from CERT Coordination Center clearly indicate securing the national information infrastructure requires vigilance and continuous efforts.[31]

Physical Threats

Physical threats to the information infrastructure include disruptions due to natural disasters—tornados, floods, earthquakes, fires, hurricanes, and ice storms—major accidents and/or terrorist activities. Any of these could destroy portions of the information infrastructure—components of the internet (e.g. any of the 13 top level servers), switching centers, telecommunications cables, satellite ground terminals, public switched networks, or disrupt energy. Past failures have led to redundancy and resilience in these infrastructures, but not immunity to catastrophic events. Most catastrophic events are confined to a particular locale and even coordinated attacks against numerous physical targets would be unlikely to disrupt the Internet, electrical supplies, or telecommunications systems for very long.

Terrorists and nation-state enemies seek to strike where it is easiest. As we enhance security against cyber threats, physical attacks become more likely. Likely targets include electrical power—transmission lines, generators and transformers—and telecommunications facilities—telecom hotels (concentrated collocation sites), signaling gateways, satellite ground stations, and transmission towers.

Electrical Infrastructure

The North American electric system supplies power through a multi-nodal, interconnected distribution system to almost all of the United States, Canada, and a portion of Baja California Norte, Mexico. Past failures concentrated industry efforts to identify points of failure and system interdependencies, and then develop backup processes, systems, and facilities.[32] This focus has made the North American electric system the world's most reliable. It is one of the greatest engineering achievements of the past 100 years, with assets valued in excess of one trillion dollars, and more than 200,000 miles of transmission lines. The system integrates almost 3,500 utility organizations serving over 100 million customers and 283 million people.[33]

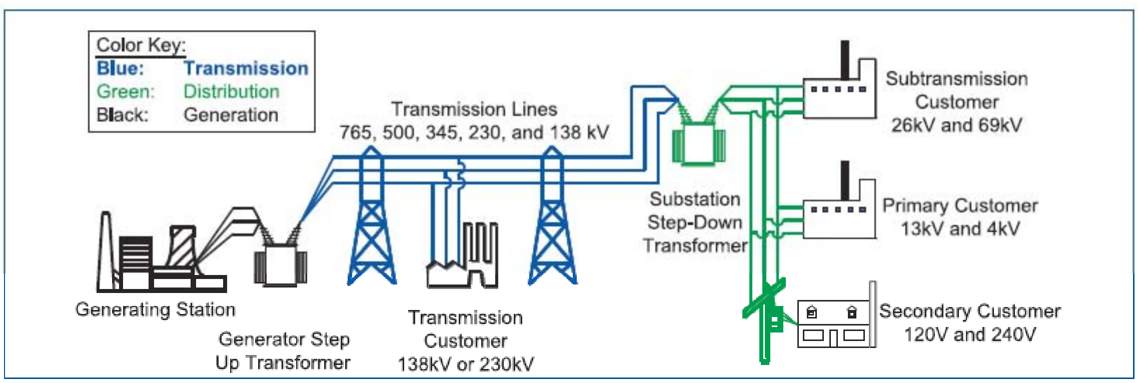


Figure 8 Basic Structure of the Electric System,
https://reports.energy.gov/B-F-Web-Part1.pdf

Although the North American power system is commonly referred to as "the grid." This grid is actually three distinct power grids or "interconnections" (Figure 9). The Eastern Interconnection takes in the eastern two-thirds of the continental United States and Canada from Saskatchewan east to the Maritime Provinces. The Western Interconnection incorporates the western third of the continental United States (excluding Alaska), the Canadian provinces of Alberta and British Columbia, and a portion of Baja California Norte, Mexico. The third interconnection encompasses most of the state of Texas. These three interconnections are electrically independent from each other.

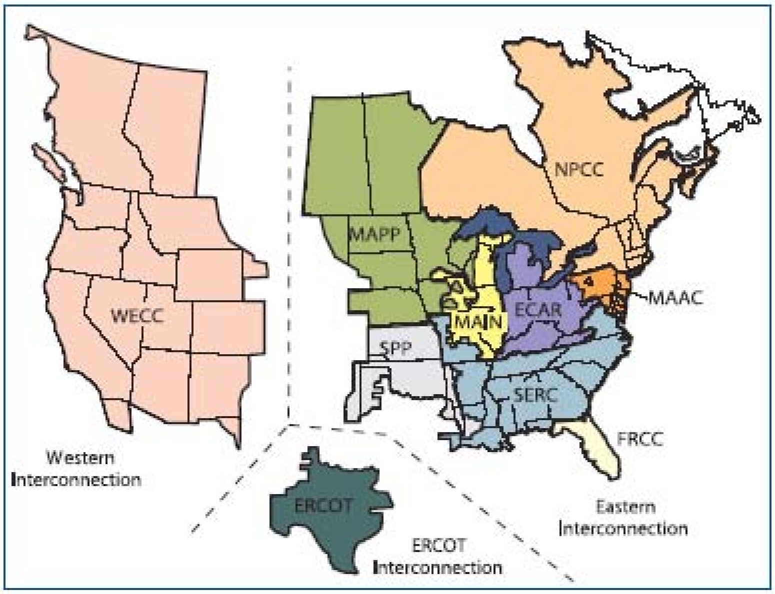


Figure 9 North American Electric Interconnection[34]

The North American Electric Reliability Council (NERC) develops standards, guidelines, and criteria to ensure electric transmission system reliability and security. Compliance with NERC standards is voluntary and not subject to government oversight. In 2003 NERC established a cyber security standard that requires electric utilities to implement cyber security processes for critical electric operations (e.g. mandated security auditing, log analysis and continual assessment). They have developed four separate cyber security guides that prescribe a proactive, ongoing process to identify and assess risk, while weighing business tradeoffs against evolving technologies and solutions. The NERC cyber security implementation plan calls for all covered entities to be in full compliance with mandated security auditing, log analysis and continual assessment by January 1, 2005.

Widespread power outages don't occur very often in the United States. However, when they do occur, they carry a significant impact. A few representative cases illustrate this point.

- August 2003: an electric power blackout impacted the eastern United States and Canada. New York City, NY, Cleveland, OH, Detroit, MI, Toronto and Ottawa, Canada all lost power when 21 power plants went down almost simultaneously. The outage affected airplanes, trains, traffic signals, elevators, web servers and even water supplies in areas distributing water via electric pumps.[35]

- *"On July 6, 1999, three days of record-breaking heat arched power lines in New York City, causing a 19-hour blackout."*

- *"On December 8, 1998, a construction crew's mistake caused a blackout across a 49-square mile area of the San Francisco Peninsula. The power went out for about 940,000 people and was restored seven hours later."*

- "On October 23, 1997, about 250,000 people in a five-mile stretch of downtown San Francisco lost power for 90 minutes or more. FBI investigators later determined someone intentionally cut the power."

- In July 1996 an electrical power blackout—traced to one 500,000-volt transmission line sagging into a tree and shorting out—affected at least 9 States in the western United States and parts of Canada and Mexico for up to 10 hours, causing airport delays and stopped subways from Denver to San Francisco. (**Cybernation**)

Part of the reason power outages are infrequent and do not last very long is that the U.S. electric power industry's security coordinators monitor large transmission networks and can perform emergency operations to redirect and restore power.

Although we can point to few incidents where a cyber attack has caused an electric power system outage, we know intuitively that electric power system attacks could be either by brute force against the physical infrastructures or a cyber attack on one of the elements of the control structure. The most likely target for a physical attack is the transmission systems—cutting major transmission lines or damaging generators—because the transmission lines spread out all over the place and any failure could lead to a major outage. The most likely target for a cyber attack is an element of the control structure. The system control centers—involved in most of the operations to stabilize the electricity network—are the most critical part of the control structure. Security coordinators, backup facilities, redundant equipment and procedures to hand-off coordination efforts minimize the threat of any attacks against the control structure.

Telecommunications Infrastructure

> "Voice and data services are provided to public and private users through a complex and diverse public-network infrastructure encompassing the Public Switched Telecommunications Network (PSTN), the Internet, and private enterprise networks (Figure 10). The PSTN provides switched circuits for telephone, data, and leased point-to-point services. It consists of physical facilities—including over 20,000 switches, access tandems, and other equipment—connected by nearly two billion miles of fiber and copper cable. The physical PSTN remains the backbone of the infrastructure, with cellular, microwave, and satellite technologies providing extended gateways to the wire line network for mobile users."[36]

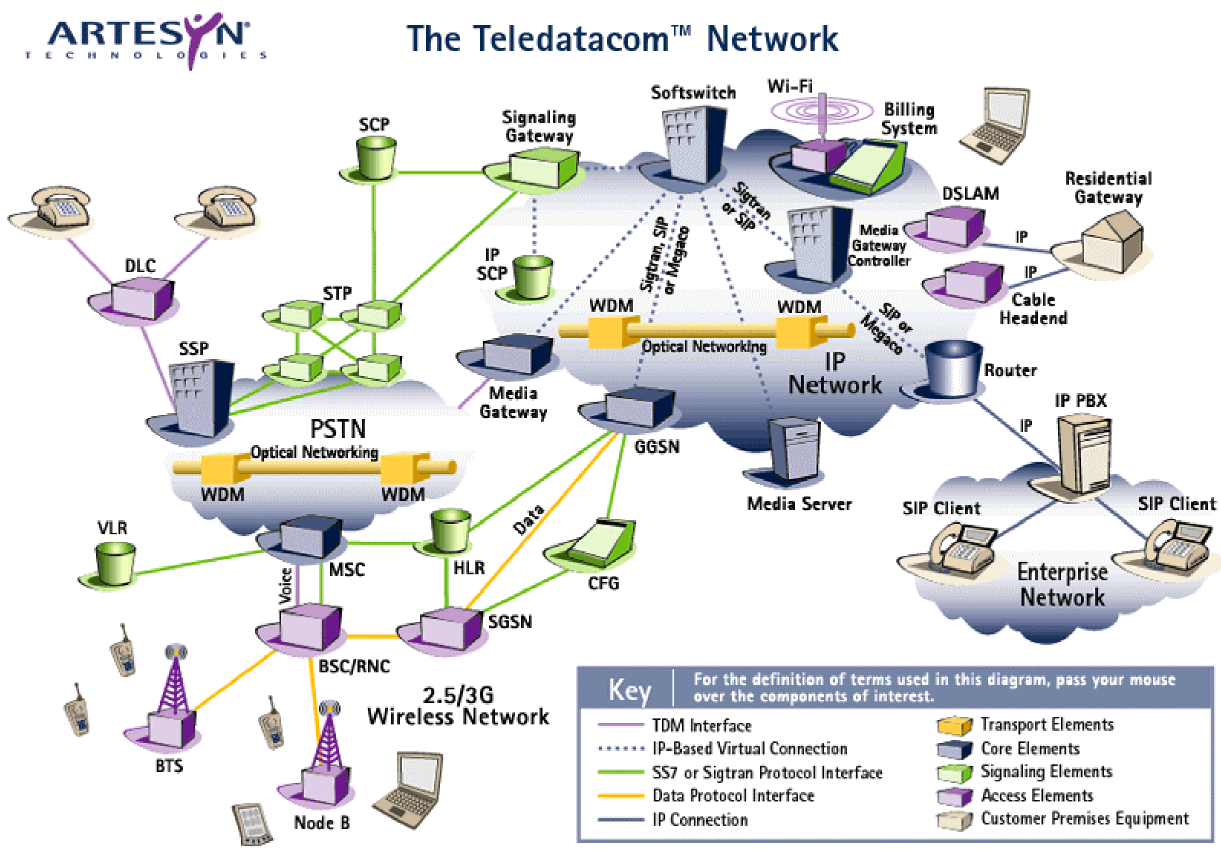


Figure 10 Teledatacom™ Diagram
Artesyn Technologies, interactive version available at
http://www.artesyncp.com/resources/teledata/

International connectivity is through 24 ocean cable systems and 70 satellite earth stations—61 Intelsat (45 Atlantic Ocean and 16 Pacific Ocean), 5 Intersputnik (Atlantic Ocean region), and 4 Inmarsat (Pacific and Atlantic Ocean regions).

"The Telecommunications Act of 1996 opened local PSTN service to competition." The Act called for existing telephone carriers to provide their competitors access to their networks. Carriers began to collect their equipment into collocation facilities, rather than putting down new cable. ISPs also moved toward these facilities to decrease costs. So, open competition, drove the PSTN and the Internet toward a posture of greater risk—interconnected, software controlled, and remotely administered—while concentrating the

physical assets into shared facilities.[37] Noticeable outages in the telecommunications network are rare, but when they occur the efforts can be far reaching.

- a few lines of defective computer code in signaling system algorithms in a software 'upgrade' resulted in 16 million people in Los Angeles, Baltimore, San Francisco, and Pittsburgh having their local telephone service interrupted in 1991.[38]

- an internal power failure at a Manhattan telephone switching center cut off half of the long distance traffic of the nation's largest long distance carrier into and out of New York City in September 1991. This switching center also carried 90% of the New York air traffic control center communications. About 400 flights were canceled and tens of thousands of passengers were inconvenienced over an eight-hour period. The outage was blamed on "a combination of equipment and human failure."[39]

Notes

[1] *The Internet and Emergency Preparedness: joint survey with Federal Computer Week magazine*, August 31, 2003, http://www.pewinternet.org/reports/pdfs/PIP_Preparedness_Net_Memo.pdf

[2] Verton, D., *Think tank: Cyberthreat overrated,* 2003, COMPUTERWORLD, http://www.computerworld.com/securitytopics/security/cybercrime/story/0,10801,77239,00.html

[3] Wallace, Bill, *Security Analysts dismiss fears of terrorist hackers: Electricity, water systems hard to damage online*, San Francisco Chronicle, June 30, 2002, http://www.sfgate.com/cgi-bin/article.cgi?file=/chronicle/archive/2002/06/30

[4] McCullagh Declan, *Perspectives: Cyberterror and professional paranoiacs*, March 21, 2003, CNET News.com, Washington D.C., http://news.com.com/2010-1071-993594.html

[5] Staniford, S., Paxsony, Vern, and Weaver, Nicholas, *How to 0wn the Internet in Your Spare Time*, *11th USENIX Security Symposium*, 2002, San Francisco, California.

[6] Libicki, Dr. M., *U.S. Foreign Policy Agenda,* USIA Electronic Journal, 1998

[7] *The National Strategy to Secure Cyberspace*, 2004

[8] *Expert: Microsoft ripe for epidemic, Associated Press*, 2004, Milwaukee Journal Sentinel Online: Cambridge, MA, http://www.jsonline.com/bym/tech/news/mar04/213097.asp

[9] Clinton, President W.J., *Critical Infrastructure Protection*, 1998, Washington D.C.

[10] Anderson, R., *Unsettling Parallels Between Security and the Environment*, 2004, http://www.sims.berkeley.edu/resources/affiliates/workshops/econsecurity/econws/37.txt

[11] Knauf, D.J., *The Family Jewels: Corporate Policy on the Protection of Information Resources*, 1991, Harvard University, Cambridge, MA, pp. vi, http://pirp.harvard.edu/pubs_pdf/knauf/knauf-p91-5.pdf

[12] ibid

Notes

[13] ibid

[14] 2003 CSI/FBI Computer Crime and Security Survey, http://www.visionael.com/products/security_audit/FBI_CSI_2003.pdf

[15] CERT/CC *Overview Incident and Vulnerability Trends*, 2004, http://www.cert.org/present/cert-overview-trends/

[16] Verton, D., *Cybersecurity Experts Urge Action*, PCWorld, December 5, 2003, http://www.pcworld.com/news/article/0,aid,113784,00.asp

[17] *The National Strategy to Secure Cyberspace*, 2004, http://www.whitehouse.gov/pcipb/physical.html

[18] The Economist: *Internet security-Combating hooligans in online space*, 2003, http://www.ebusinessforum.com/index.asp?layout=rich_story&doc_id=6869

[19] http://www.cert.org/present/cert-overview-trends/module-2.pdf, page 18

[20] *The National Strategy to Secure Cyberspace*, 2004

[21] Carnegie Mellon University Software Engineering Institute, *Overview of Attack Trends,* 2002, CERT® Coordination Center

[22] Office of Science and Technology Policy, National Security and International Affairs Division., *Cybernation: The American Infrastructure in the Information Age: A Technical Primer on Risks and Reliability*, 1998, http://www.fas.org/irp/threat/980107-cyber2.html

[23] ibid

[24] ibid

[25] Staniford, S., Paxsony, Vern, and Weaver, Nicholas. *How to 0wn the Internet in Your Spare Time,* in *11th USENIX Security Symposium*. 2002, San Francisco, California, http://www.itsecurity.com/papers/sildef1.htm

[26] Office of Science and Technology Policy, National Security and International Affairs Division., *Cybernation: The American Infrastructure in the Information Age: A Technical Primer on Risks and Reliability*, 1998, http://www.fas.org/irp/threat/980107-cyber2.html

[27] ibid

[28] Wheeler, D.A., *The right mentality is half the battle*, 2003, http://www-106.ibm.com/developerworks/linux/library/l-sp1.html

[29] Shelton, D., *Banks appease online terrorists*, The Net, 1996, http://news.com.com/2100-1023-213603.html?legacy=cnet

[30] The Economist: *Internet security-Combating hooligans in online space*, 2003, http://www.ebusinessforum.com/index.asp?layout=rich_story&doc_id=6869

[31] Cross, S.E., *Cyber Security*, in Senate Armed Services Committee Subcommittee on Emerging Threats and Capabilities, 2000

[32] *The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets*, 2003, http://www.whitehouse.gov/pcipb/physical.html

[33] U.S.-Canada Power System Outage Task Force *Final Report on the August 14, 2003 Blackout in the United States and Canada: Causes and Recommendations*, April 2004, Task Force Co-Chairs Spencer Abraham, Secretary of the U.S. Department of Energy (USDOE) R. John Efford, Canadian Minister of Natural Resources (current) and Herb Dhaliwal (August-December 2003), https://reports.energy.gov/B-F-Web-Part1.pdf

Notes

[34] U.S.-Canada Power System Outage Task Force *Final Report on the August 14, 2003, Blackout in the United States and Canada: Causes and Recommendations*, April 2004, p. 6, https://reports.energy.gov/B-F-Web-Part1.pdf

[35] CNN.COM/US, *(CNN) Major power outage hits New York, other large cities*, 2003, http://www.cnn.com/2003/US/08/14/power.outage/

[36] *The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets*, 2003, pp. 47-48

[37] Ibid

[38] Office of Science and Technology Policy, National Security and International Affairs Division., *Cybernation: The American Infrastructure in the Information Age: A Technical Primer on Risks and Reliability*, 1998, http://www.fas.org/irp/threat/980107-cyber2.html

[39] Ibid.

Chapter 4

What has the nation done?

Laws too gentle are seldom obeyed; too severe, seldom executed.

—Benjamin Franklin

Even though the government does not own, operate or maintain the majority of the networks intertwined in the Internet it does rely heavily on systems interfaced to the Internet for national defense, continuity of government, public awareness and education. The government continues a significant effort to protect the portions of the Internet it does operate, maintain, control and rely upon. Setting the example is an essential first step. The government has already taken an active role in developing and protecting the Internet—commissioning the beginnings of the Internet (ARPANET), funding research and development, establishing national policy, pushing for standards, passing related legislation, developing government-private sector partnerships and educating individual users. The government created a National Cyber security Division under DHS to serve as the federal government's cyber security focal point for public and private sectors.

The Administration established a Presidential cyber security advisor. This person resides within the Homeland Security Council and runs a staff dedicated to protection of our nation's critical infrastructure. The President signed Homeland Security Presidential Directive -7 on December 17, 2003 that created a Policy Coordinating Committee to make sure all the different elements of the federal government are working together on cyber security.

National efforts, so far, have balanced calls to for strong government action with a belief in 'the market' to bring about essential, stabilizing security initiatives.

Chapter 5

What are the nation's options for the future?

> *That government is best which governs the least, because its people discipline themselves.*
>
> —Thomas Jefferson

The problems are real. The nation must act. The methods the nation has at its disposal include: establishing policy, increasing the focus on security, mandatory standards, laws, education and partnerships with the private sector. Except in the standards arena, there don't appear to be any workable methods to follow Jefferson's advice.

Policy

One of the most recent policy documents providing direction for protecting the NII is The National Strategy to Secure Cyberspace, released February 2003. This strategy lays out five national priorities including: 1) a National Cyberspace Security Response System; 2) a National Cyberspace Security Threat and Vulnerability Reduction Program; 3) a National Cyberspace Security Awareness and Training Program; 4) Securing Governments' Cyberspace; and 5) National Security and International Cyberspace Security Cooperation.

It has been criticized for relying on market forces and private cooperation rather than directing software vendors and others to provide security. Since security measures are designed to prevent disaster rather than produce profit, accountability must be at the center of security. Extending and clarifying policy to clearly establish security accountability for specific levels of activity—software vendors, corporations, ISPs, network administrators, and individual users should be examined. Policy, however, is an evolutionary process—make, implement, evaluate, repeat.

Security

If it's not secure, the national information infrastructure is unusable for most activities. Security problems arise from a wide variety of issues—software flaws, hardware insecurities, poor management practices and administration procedures, and user apathy. Government can use its influence to raise the priority of cyber security to one of national (and international) importance, allocate additional funds to research and develop essential security measures, re-emphasize user education.

System and network operators must be fiscally judicious in the security measures they implement. Security measures are not free. Most corporations have not been the target of serious cyber attacks, so the payoff for security investments is difficult to quantify and justify. No matter how effective information security programs, procedures and equipment become it is impossible to eliminate all threats.

Establishing incentives to encouraging promptly fixing problems, installing patches and remediation of known vulnerabilities and disincentives for those who do not, might significantly reduce exploits and make it more difficult to attack our networks.

Increased research and development grants and partnerships focusing on developing new robust, secure capabilities may help the nation stay ahead of those with the capabilities and intent to do harm to our critical infrastructures.

Security measures are not strictly technical measures. Computer networks require trusted individuals to install, operate and maintain them. "Insider" violations of the trust placed in them can (and often do) result in some of the most serious incidents encountered. Only a system of checks and balances that brings attention to out of the ordinary activities can root out "insiders" with evil intent.

Existing laws, rules, and regulations (e.g. Clinger-Cohen Act, Government Performance and Results Act, Government Paperwork Elimination Act, and Federal Information Security Management Act) refer to information technology performance measurement in general, and security performance measurement specifically, as a requirement. The government uses NIST Special Publication 800-55, Security Metrics Guide for Information Technology Systems, as its guideline for measuring information technology security performance and ensuring it meets regulatory, financial, and organizational standards for security controls, policies, and procedures.

Of course, it is imperative for the government to lead by example. Every year the House Government Reform Committee's Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census releases a "Computer Security Report Card" on federal agencies. In the December 2003 "Report Card," 8 of 24 Federal Agencies received a failing grade and only 7 received a grade of 'C' or better.

Meanwhile the industry software leader, Microsoft indicates they are focused on security. Founder, Bill Gates said, "Windows XP SP2 (expected to ship mid-year 2004) is a release totally focused on security." This focus must become universal, extending throughout the national information infrastructure so everyone remains focused on security.

Standards

Internet standards, for the most part, have not been mandated by government but rather developed by groups such as IETF, ISOC, ANSI, ISO, IEEE, IEC, and ITU-T whose standards become such through wide-spread adaptation and use. Government must continue to encourage generic open information systems platforms and processes, promote open technology transfers among a wide range of innovators, developers, security experts and users, and encourage a competitive marketplace.

The Internet Engineering Task Force (IETF) is a self-organized group that contributes to engineering and evolution of Internet technologies. They develop open standards. In November 2003, they released Internet Official Protocol Standards, STD-001[1] which contains a snapshot of the state of standardization of protocols used in the Internet as of October 2, 2003.

Throughout industry there is discouragement for government setting specific standards for information security and encouragement for market driven standards. Harris N. Miller, President, Information Technology Association of America (ITAA), in testimony before a Senate Subcommittee on Technology, Terrorism and Government Information said the industry, discouraged the setting of 'standards' because they tend to be only a snapshot of technology at a given moment and they risked stopping the progress of technology rather than encouraging ongoing development of best practices and de facto standards in response to market place demand.[2]

Laws

The laws and legislation in the United States are currently not up to the task of regulating or establishing accountability or liability for electronic attacks. Should the companies who create the software be liable for lost or corrupted data resulting from deficient designs and vulnerabilities of their products? What about the agencies charged with oversight and watchdog efforts on the Internet—should they be responsible or liable for these vulnerabilities? What responsibilities does the consumer have?

Executive orders and Presidential Commissions have laid out policies and direction. We have a wide range of laws applicable to various computer security and privacy issues.

- **Computer Security Act of 1987** (January 1988): improve security and privacy of sensitive information in Federal computer systems and establish minimum acceptable security practices;
- **Information Technology Management Reform Act** (1996) aka Clinger-Cohen Act: improve government performance through the effective application of information technology;
- **Child On-Line Protection Act** (1998): restrict access by minors to materials commercially distributed by means fo the world-wide-web that are harmful to minors;
- **US PATRIOT Act** (October 2001): To deter and punish terrorist acts in the US and around the world—sections deal with issues of computer fraud, abuse and trespass;
- **The Computer Fraud and Abuse Act** (amended in 1994, 1996 and Section 1030 in 2001 by the US PATRIOT Act) raised maximum penalty for hackers, clarified intent to do damage vice particular consequences/damages, aggregated hackers entire conduct, and redefined loss;
- **Sarbanes-Oxley Act** (January 2002): CEOs personally validate financial statements and attest to the company having proper internal controls (requires secure IT systems);
- **Cyber Security Enhancement Act of 2002** aka Homeland Security Act Amendments Section 225: amends Federal sentencing guidelines for crimes that are related to fraud or unauthorized access to federal government computers and restricted data; establishes a National Infrastructure Protection Center; allows ISPs to make emergency disclosures of records to a government entity;
- **HIPAA** (1996; implemented April 2003): federal privacy standards to protect patients' medical records and other health information (health care);
- **CAN-SPAM Act of 2003:** requires unsolicited commercial e-mail messages to be labeled and include opt-out instructions and the sender's physical address;

- **Financial Modernization Act of 1999** aka Gramm-Leach-Bliley Act**:** privacy policy on sharing non-public personal information, requires notice and "opt-out" opportunity before sharing of non-public personal information (financial services);
- **Federal Trade Commission Act 1914** (as amended): regulate unfair advertising and deceptive practices;

There are numerous cyber security laws pending. A July 2003 report released by the National Conference of State Legislatures (NCSL), indicates, at least 24 states have introduced bills and 10 states have passed laws addressing information security since fall 2001. States with new statutes included: Florida, Michigan, California, Illinois, Kansas, Nevada, South Carolina, Tennessee, Texas and Virginia.

Recent court proceedings illustrate the need for corporate practices that establish objective measures of the effectiveness of their network security plans. Corporations are required to set up and document the steps taken to develop and employ a secure network design, show continuing measures to maintain the security, ensure the strength of network maintenance and security monitoring actions. But this may not be enough!

When things go wrong on the national information infrastructure, who is liable? Who should be held accountable for problems?

It's not just the 'bad guys' who should be held responsible for security-related software failures. Software manufacturers and software consumers are also to blame for sloppy software design and lax system administration. The government's primary response has been an attempt to deter hackers.

Laws need to clearly establish redress and accountability. However, some laws seem to impede information security and national information infrastructure protections. The Uniform Computer Information Transactions Act (UCITA)[3] blocks software publisher and on-line services liability for security related software defects—even when the defect(s) are known and not disclosed to the purchaser.

The government has not clearly identified avenues for redress and accountability when the information infrastructure—software and hardware—fail to carry out their assigned tasks. The nation should clarify existing "defective product" laws as they apply to software. How? Legislative responses—such as increasing the liability of software and system vendors and system operators for system insecurities and directing mandatory reporting of security breaches that could threaten the national information infrastructure—could help to overcome the apparent failure of existing incentives and move the market to respond adequately to the security challenge.[4]

If our government passed legislation to place responsibility and liability for Internet security upon software and hardware developers, ISPs, corporations and individuals we could see a significant increase in protective measures developed and implemented. For example, holding parties liable for not securing their facilities against being used serendipitously as part of a DDOS attack would increase the business incentive for security investment. Simultaneously, government must take the lead to create private sector incentives establishing and maintaining a secure environment for essential Internet activities to operate—that is carefully balance laws and regulations to ensure we don't erect roadblocks to technology development.

Government-Industry partnerships

The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets calls for collaborative partnerships between various governmental agencies and the private sector to provide a foundation for developing and implementing coordinated protection strategies. Both government and the private sector have established a variety of security focused partnerships and organizations.

Philip Reitinger, Senior Security Strategist for Microsoft stressed the necessity for partnerships and information sharing, in testimony before the House Select Committee on Homeland Security on July 15, 2003. He said, "without a multidisciplinary effort by both government and industry, we will not succeed" in protecting our cyber networks.[5] The Department of Homeland Security (DHS) established the National Cyber Security Division (NCSD) in June 2003. Press releases indicated NCSD would be responsible for identifying, analyzing and reducing cyber threats and vulnerabilities; disseminating threat warning information; coordinating incident response; and providing technical assistance in continuity of operations and recovery planning

The National Cyber Security Division created the US-CERT program in September 2003. US-CERT, a partnership between DHS and the private sector (Carnegie Mellon University Software Engineering Institute), is charged with protecting our nation's Internet infrastructure by coordinating defense against and response to cyber attacks, consolidating available information and providing it to individuals and organizations in a timely, understandable way. They developed a National Cyber Security Alert System to send out 'Alerts' outlining the steps and actions corporate and home computer users can take to protect themselves from attack.[6] The National Cyber Security Division established a National Cyber Security Alert System (NCSD), under US-CERT in January 2004, to keep consumers informed of security hazards and to provide e-mail updates upon request. NCSD is tasked to coordinate cyber security activities within DHS and other agencies and to serve as the focal point for contact with the private sector.

The Information Technology Information Sharing and Analysis Center (IT-ISAC) was founded in January 2001 by nineteen prominent IT industry companies (including

Oracle, IBM, EDS, and Computer Sciences). The group modeled the Financial Services Information Sharing and Analysis Center (FS-ISAC) to establish a professional association, completely separate from government. The group shares information about security attacks and vulnerabilities among all the members. Member companies report security problems they encounter or solutions they identify. The information is distributed anonymously to increase information sharing among traditionally competitive companies whose organization specific security information has been closely guarded.[7]

The Cyber Security Industry Alliance (CSIA), initiated in February 2004, is focused on improving cyber security through public policy initiatives, public sector partnerships, corporate outreach, academic programs, alignment behind emerging industry technology standards and public education.[8]

In testimony before the Senate Subcommittee on Technology, Terrorism and Government Information Hearing on *Cyber Attacks: Removing Roadblocks to Investigation and Information Sharing*, March 28, 2000, of Harris N. Miller, President, Information Technology Association of America (ITAA), outlined the Associations plan for an offensive against cyber attacks—"exploring joint research and development activities, international issues, and security workforce needs." The plan included awareness, education, training, best practices, research and development, international coordination, and information sharing.

When it comes to sharing sensitive security information—especially when companies are seeking to maintain privacy—there seems to be a propensity for private sector only partnerships. Private corporations believe excluding government provides greater anonymity.

What are the ongoing and unresolved issues?

At a June 2003, Critical Infrastructure Protection Project[9] *Critical Conversations* forum session, Mr. John Derrick, Chairman of the Board and former CEO of Pepcom Holdings, Inc. said, *"There are three overarching questions. One, what should be done? Two, who pays? And three, who decides the first two?"*[10]

Here are a few more questions. Can all the applications and infrastructure encompassed by the national information infrastructure be protected? Who should protect it? Why? Should government provide oversight or hands-on day-to-day involvement? Do we need to legislate protections for software liability? Should there be an industry 'watch dog'? Should we eliminate anonymity from the Internet? Should we give up privacy to gain security? Should the government offer rewards for the capture and conviction of individuals or groups responsible for introducing malicious code on to the Internet? The answers change depending on whom you ask.

It should be obvious that everything cannot be protected. Finite resources and the relative cost versus benefit must be factored into the equation. Protection must be a shared responsibility but those who own, operate, maintain and use the networks must implement the majority of protective measures. Since the risks—data loss, system outages, lost business, liability, etc.—are theirs, implementation is an associated operation expense.

Private partnerships, information technology associations and standards organizations are initiating a multi-disciplinary approach to confront the threats. The government should continue in an oversight and coordination role. Continuing to expand the cooperative efforts of DHS and US-CERT can function to provide oversight to the disperse efforts at combating attacks against the national information infrastructure.

Cyber Legislation is a balancing act between evolving technologies and legal responsibilities. The law always lags the development. Several areas worth considering include liability for security flaws, issuing a single, multi-jurisdictional warrant so investigators can track and identify intruders, federal licensing for private computer investigators compelling them to report information they find on intruders to the federal government, and waiving the Employee Polygraph Protection Act (similar to existing exemptions under sections 2006 and 2007 for government employees, national defense and security, etc.) to allow firms to monitor information security personnel.[11] The information technology private sector believes market driven standards and regulation is more appropriate than mandatory direction from Congress. Paul Kurtz, CSIA Executive Director, said, “We believe regulation can’t be the primary means of … cyber security.”[12] But even without new legislation addressing security flaws, as the impact of the attacks increase in magnitude, we will, no doubt, see increased suits against software manufacturers for the harms suffered from the security failures and against third parties who fail to properly implement security initiatives.

Government rewards or bounties might lead to the capture and conviction of some of the perpetrators and discourage others. Of course, Microsoft has already offered rewards for the individuals responsible for various viruses and worms—e.g. January 2004 offered $250,000 for information leading to the capture and conviction of the individual or group responsible for the release of MyDoom.B (The SCO Group[13]—target of the original MyDoom virus—also offered a $250,000 reward); MS also offered $250,000 rewards for capture/conviction of those responsible for MSBlast worm and Sobig.F virus without results.

The federal government is already using its procurement power to demand increased security in the software it procures. A procurement program called SmartBuy initiated in 2003 to consolidate software purchases should help federal agencies negotiate terms to enhance cyber security, reduce prices and improve contractual terms. The Department of Energy (along with the U. S. Department of Homeland Security, the National Security Agency, the Defense Information Systems Agency and the U.S. General Services Administration) took the first step in a September 2003 contract with Oracle, requiring database software be delivered preconfigured to the highest security settings built around a set of security benchmarks.[14]

Final Thoughts

Engineers seek technical fixes and politicians seek legislated fixes. In reality, however neither of these will take care of all the possibilities. There is no perfect solution. The choices are often uncomfortable, each good but opposed … Ignore it—too much hype; too little problem? Do everything—continuous technical fixes and lots of legislation? Too expensive? Prioritize?

The national information infrastructure is 'only as secure as the weakest link.' Often the weakest links in the NII chain are the individual, poorly protected computer and the careless user. Nefarious characters will continue to seek out methods and means to attack, steal, and seize control, etc. through the easiest methods they can find. A few things to keep in mind:

- Baseline security features should be automatically enabled at installation

- Current laws criminalize hacking, theft and destruction
- Efforts need to continue trying to resolve the issues associated with sharing problem and solution information
- Private sector owns and operates the majority of the infrastructure and has the majority of the knowledge and expertise, so they should continue to develop market driven, industry led security solutions
- Only by sharing information with law enforcement and appropriate industry groups will we be able to identify and prosecute cyber criminals, identify new cyber security threats and prevent successful attacks on our critical infrastructures and economy.[15]
- Any legislation placing additional responsibility and liability for Internet security upon software and hardware developers, ISPs, corporations and individuals should be complemented by incentives (e.g. tax breaks and subsidies) to encourage the private sector to establish and maintain a secure environment for essential Internet activities to operate
- Insurance companies are trying to develop software security actuarial tables and identify security measures to mitigate risks, such as a set of best practices and established security standards; e.g. Lloyd's of London is offering a 10% premium discount when Tripwire software is properly deployed on the networks[16]

Harris Miller, president of the Information Technology Association of America, (ITAA), representing over 400 companies in the information technology (IT) industry, sums up the battle for cyber security this way, "*The constant challenge is that it's a constant challenge"*... and it won't end any time soon.

Notes

[1] IETF STD-001, 2003, ftp://ftp.rfc-editor.org/in-notes/rfc3600.txt

[2] Testimony of Harris N. Miller, President, Information Technology Association of America (ITAA), Before the Senate Subcommittee on Technology, Terrorism and Government Information Hearing on *Cyber Attacks: Removing Roadblocks to Investigation and Information Sharing*, March 28, 2000

[3] Additional information at: http://www.ala.org/ala/washoff/WOissues/copyrightb/ucita/states.htm

[4] *Cyber Security Today and Tomorrow: Pay Now or Pay Later*, Computer Science and Telecommunications Board, 2002, http://www.cstb.org

[5] *America at Risk: Closing the Security Gap*, February 2004, prepared by Democratic members of the House Select committee on Homeland Security, Jim Turner, Ranking Member, http://www.house.gov/hsc/democrats

[6] Current Alerts can be viewed at: http://www.us-cert.gov/channels/

Notes

[7] Information Technology Information Sharing and Analysis Center Home Page, https://www.it-isac.org/

[8] Cyber Security Industry Alliance, http://www.csialliance.org/

[9] *Protecting America's Critical Infrastructure: From War Room to Boardroom*, June 18, 2003, CIP Project forum panel discussion at George Mason University, http://techcenter.gmu.edu/programs/conferences/npc_jun03_transcript.pdf

[10] Ibid.

[11] John Moteff, Specialist in Science and Technology Science, Technology, and Medicine Division, *CRS Report for Congress: Critical Infrastructures: A Primer*, http://www.fas.org/irp/crs/98-675.pdf

[12] Keith Ward, ENTmag.com News, *New Association to Raise Cyber Security Awareness*, February 25, 2004, San Francisco

[13] owner of the UNIX® operating system, http://www.caldera.com/company/

[14] http://www.cisecurity.org/bench.html

[15] CIO Cyberthreat Response & Reporting Guidelines, http://www.cio.com/research/security/incident_response.pdf

[16] In 2001, the average annual cyber policy premium was $45,000 with a $10 million liability limit

Glossary

AFFP	Air Force Fellows Program
AKA	Also Known As
ANSI	American National Standards Institute
AU	Air University
AWC	Air War College
CAN-SPAM	Controlling the Assault of Non-Solicited Pornography and Marketing Act
CERT/CC	Computer Emergency Response Team/Coordination Center
CHIPS	Clearing House Inter-bank Payments System
DOD	Department of Defense
HIPAA	Health Insurance Portability and Accountability Act
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
ISO	International Organization for Standardization
ISOC	Internet Society
ITU-T	International Telecommunication Union - Telecommunication Standardization Sector
NIST	National Institute of Standards and Technology
NCSD	National Cyber Security Division
SWIFT	Society for Worldwide Internet Financial Telecommunications
UCITA.	Uniform Computer Information Transactions Act
USAF	United States Air Force

Definitions

http://www.webopedia.com and http://searchsecurity.techtarget.com/sDefinition/

American National Standards Institute. A private, non-profit organization (501(c)3) that administers and coordinates the U.S. voluntary standardization and conformity assessment system.

Anti-virus software. Not foolproof. Antivirus software regularly fails to detect newly discovered viruses. Examples include *Melissa*, *ExploreZip*, *MiniZip*, *BubbleBoy*, *ILoveYou*, *NewLove*, *KillerResume*, *Kournikova*, and *NakedWife*.

authentication. The process of identifying an individual, usually based on a username and password. Authentication merely ensures that the individual is who he or she claims to be so all parties know who they are dealing with at the outset of an electronic exchange. Authentication does not provide information about the access rights of the individuals.

CERT/CC. Computer Emergency Response Team/Coordination Center is a partnership between DHS and Carnegie Mellon University Software Engineering Institute.

CHIPS. Clearing House Interbank Payments System is a bank-owned payments system for clearing and settling large value payments. CHIPS processes over 257,000 payments a day with a gross value of over $1.3 trillion. It is a premier payments platform serving the largest banks from around the world, representing 22 countries world wide, processing over 95% of the USD cross-border payments.

computer. An electronic machine that performs high-speed mathematical or logical calculations or that assembles, stores, correlates, or otherwise processes and prints information derived from coded data in accordance with a predetermined program.

crackers. Individuals who's aim is to sneak through security systems to break into computer systems; term was coined in the mid-80s by hackers to differentiate themselves from individuals whose sole purpose is to sneak through security systems. Also applied to those who copy commercial software illegally by breaking (cracking) the various copy protection and registration techniques being used.

DHS. Department of Homeland Security, established by …

Domain Name System. An Internet service that translates domain names into IP addresses. "Mnemonic" domain names are easier to remember than numeric IP addresses. Since the Internet however is based on IP addresses, a DNS service must translate every domain name into the corresponding IP address. For example, the domain name www.example.com might translate to 198.105.232.4. Domain names are also used for reaching e-mail addresses and for other Internet applications.

hackers. Individuals more interested in gaining knowledge about computer systems and possibly using this knowledge for 'playful' pranks. You don't have to be a genius to hack into a computer. Hacking actually takes very little technical knowledge because any search engine queried about "hacking tools" will list numerous sites that provide downloadable tools and even directions.

ICMP. Short for ***I**nternet **C**ontrol **M**essage **P**rotocol,* an extension to the Internet Protocol (IP) defined by RFC 792. ICMP supports packets containing error, control, and informational messages.

integrity. Refers to the validity of the data, that is a message or data cannot be changed in transit.

malware. Short for malicious software; it is software designed specifically to damage or disrupt a system, such as a virus or a Trojan horse.

NCSD. National Cyber Security Division, a Division of DHS charged with …

non-repudiation. assurance that a transferred message has been sent and received by the parties claiming to have sent and received the message. Non-repudiation is the 'guarantee' that the sender of a message cannot later deny having sent the message and that the recipient cannot deny having received the message.

phishers. Hackers 'phishing' (sometimes called carding or brand spoofing) to steal your information. They imitate legitimate companies in e-mails to get people to share their passwords and credit card numbers. Recently imitated companies include Charlotte's Bank of America, Best Buy and eBay whose customers were directed to Web pages nearly identical to the company sites, where they were asked for account and other personal information.

ping. A utility used to determine whether a specific IP address is accessible. It sends a packet to the specified address and waits for a reply. PING is used primarily to troubleshoot Internet connections.

privacy. Ensuring details of an electronic transaction remain between the involved parties.

root servers. The root servers contain the IP addresses of all the TLD registries – both the global registries such as .com, .org, etc. and the 244 country-specific registries such as .fr (France), .cn (China), etc. This is critical information. If the information is not 100% correct or if it is ambiguous, it might not be possible to locate a key registry on the Internet.

routers. The computer switching circuits that direct internet traffic to its destination.

sandboxing. A security application that runs unknown (or potentially unkown, i.e. trojanned) software in an isolated environment before allowing it to run on the host.

smurfing. A type of network security breach where a network connected to the Internet is flooded with replies to ICMP echo (PING) requests. The smurf attacker sends PING requests to an Internet broadcast address using the spoofed address of the attacker's victim. All the hosts receiving the PING request reply to this victim's address instead of the real sender's address. A single attacker sending hundreds or thousands of these PING messages per second can fill the victim's access line with replies, and potentially bring the entire Internet service to its knees.

Spoofing. A technique used to gain unauthorized access to computers, whereby the intruder sends messages to a computer with an IP address indicating the message is coming from a trusted host. To engage in IP spoofing, a hacker first finds an IP address of a trusted host and then modifies the packet headers so it appears the packets are coming from that host.

surreptitious worms. These spread more slowly, but in a much harder to detect "contagion" fashion, masquerading as normal traffic.

SWIFT. Society for Worldwide Internet Financial Telecommunications is the world's largest financial payments network. It is an industry owned, cooperative that provides messaging services to banks, broker-dealers, and investment managers as well as to market infrastructures in payments, treasury, securities, and trade. It also acts as a standards body for messaging protocols in these areas. SWIFT processes over $6 trillion of risk-bearing messages per day, for 7,500 member institutions (banks and national payment associations) in 197 different countries.

Trojan. A destructive program that masquerades as a benign application. Unlike viruses, Trojans do not replicate themselves but they can be just as destructive. One of the most dangerous types of Trojan is a program that claims to rid your computer of viruses but instead introduces viruses onto your computer.

UCITA. Uniform Computer Information Transactions Act is not federal law but a proposed uniform law for each state to consider enacting. Two states -- Maryland and Virginia -- have enacted different versions of it.

virus. A program or piece of code that is loaded onto your computer without your knowledge and runs against your wishes. Viruses can also replicate themselves. All computer viruses are manmade. A simple virus that can copy itself over and over again is relatively easy to produce. Even such a simple virus is dangerous because it will quickly use all available memory and bring a system to a halt. Some people distinguish between general viruses and *worms.*

web bugs. Also called a *Web beacon* or a *pixel tag* or a *clear GIF.* Used in combination with cookies, a *Web bug* is often a transparent graphic image, usually no larger than 1 pixel x 1 pixel, placed on a Web site or in an e-mail and used to monitor the behavior of the user visiting the Web site or sending the e-mail.

World Wide Web. All of the publicly accessible web sites in the world, in addition to other information sources that web browsers can access, that support specially formatted documents. The documents are formatted in a markup language called HTML (*HyperText Markup Language*) that supports links to other documents, as well as graphics, audio, and video files. This means you can jump from one document to another simply by clicking on hot spots. The other sources include FTP sites, USENET newsgroups, and a few surviving Gopher sites. Note all Internet servers are not part of the World Wide Web.

Worm. Automated intrusion agent; a special type of virus that can replicate itself and use memory, but cannot attach itself to other programs.

Bibliography

Anderson, Ross. *Unsettling Parallels between Security and the Environment*, 2004, Available from http://www.sims.berkeley.edu/affiliates/workshops/econsecurity/econws/37.txt.

Byon, Imju. "Survivability of the U.S. Electric Power Industry" Master of Science in Information Networking, Carnegie Mellon University Information Networking Institute, 2000

Computer Emergency Readiness Team (CERT) Coordination Center, *Overview Incident and Vulnerability Trends*, 2004

Cia World Factbook: United States, 2002 Federal Information and News Dispatch, Inc., January 1, 2002 Available from http://80-web.lexis-nexis.com.ezp2.harvard.edu/universe/document?_m=9afad8e9ba0f0e1c52d8931db089c7bd&_docnum=3&wchp=dGLbVzz-zSkVb&_md5=d9d7449d35167d271e7a29f98f9854fd.

Clinton, President William J. *Critical Infrastructure Protection*, 1998. Available from http://www.fas.org/irp/offdocs/pdd/pdd-63.htm.

CNN.COM/US. (AP) *Last Major Blackout Was 7 Years Ago* August 14, 2003, 2003. Available from http://www.cnn.com/2003/US/08/14/previous.blackouts.ap/index.html.

(CNN) Major Power Outage Hits New York, Other Large Cities, 2003. Available from http://www.cnn.com/2003/US/08/14/power.outage/

Princeton Survey Research Associates, *The Internet and Emergency Preparedness: A Joint Survey with Federal Computer Week Magazine*, 2003, http://www.pewinternet.org/reports/pdfs/PIP_Preparedness_Net_Memo.pdf.

The Constitution of the United States.

Senate Armed Services Committee Subcommittee on Emerging Threats and Capabilities, *Cyber Security*, March 1, 2000

Cyber-Security Today and Tomorrow: Pay Now or Pay Later, edited by Computer Science and Telecommunications Board. Washington, D.C.: National Academy Press, 2002

Department of Defense Critical Information Infrastructure Protection Plan, 1998

The Economist: Internet Security-Combating Hooligans in Online Space, 2003. Available from http://www.ebusinessforum.com/index.asp?layout=printer_friendly&doc_id=6869.

Executive Order 13010. July 15, 1996.

Expert: Microsoft Ripe for Epidemic, Associated Press Milwaukee Journal Sentinel Online, March 8, 2004, 2004. Available from http://www.jsonline.com/bym/tech/news/mar04/213097.asp.

Carnegie Mellon University Software Engineering Institute, *Overview of Attack Trends* CERT® Coordination Center, 2002. Available from http://www.cert.org/archive/pdf/attack_trends.pdf.

Kahn, Robert E. and Cerf, Vinton G. *Internet History, What Is the Internet (and What Makes It Work)* December, 1999, 1999. Available from http://global.mci.com/us/enterprise/insight/cerfs_up/internet_history/whatIs.xml.

Knauf, Daniel J. "The Family Jewels: Corporate Policy on the Protection of Information Resources." pp. vi. Harvard University, Cambridge, MA, 1991.

Libicki, Dr. Martin. "U.S. Foreign Policy Agenda." *USIA Electronic Journal* 3, no. 4 (1998).

McCullagh, Declan. *Perspectives: Cyberterror and Professional Paranoiacs,* CNET News.com, 2003. Available from http://news.com.com/2010-1071-993594.html.

The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets, 2003, pp. 47-48, Available from http://www.dhs.gov/interweb/assetlibrary/Physical_Strategy.pdf.

The National Strategy to Secure Cyberspace, 2004, Available from http://www.whitehouse.gov/pcipb/executive_summary.pdf.

Office of Science and Technology Policy, National Security and International Affairs Division. *Cybernation: The American Infrastructure in the Information Age*, 1998.

Presidential Decision Directive/NSC-63, Critical Infrastructure Protection, May 22, 1998.

Protecting America's Critical Infrastructures: From War Room to Board Room, The CIP Report 2, no. 1, 2003.

Richardson, Robert. *2003 CSI/FBI Computer Crime and Security Survey*.

Shelton, Denise. *Banks Appease Online Terrorists,* June 3, 1996, 1996. Available from http://news.com.com/2100-1023-213603.html?legacy=cnet.

Staniford, Stuart, Paxsony, Vern, and Weaver, Nicholas. *How to 0wn the Internet in Your Spare Time*, Paper presented at the 11th USENIX Security Symposium, San Francisco, California, August 8, 2002.

Verton, Dan. *Cybersecurity Experts Urge Action*, Computerworld, December 05, 2003.

Think Tank: Cyberthreat Overrated COMPUTERWORLD,, January 3, 2003, 2003. Available from http://www.computerworld.com/securitytopics/security/cybercrime/story/0,10801,77239,00.html.

Wallace, Bill. *Security Analysts Dismiss Fears of Terrorist Hackers: Electricity, Water Systems Hard to Damage Online*, San Francisco Chronicle, June 30, 2002.

Wheeler, David A. *The Right Mentality Is Half the Battle,* August 21, 2003.